Kentucky.gov

Commonwealth
Office of Technology

From: Ritchey, Gail (COT)
Sent: Wednesday, July 23, 2008 2:44 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: COT Security Alert: DNS Server Vulnerability

COT Security Alert

The Commonwealth Office of Technology (COT) has received the alert shown below concerning vulnerabilities in the DNS protocol that may allow an attacker to redirect web site traffic to alternate web sites. Various DNS software updates for mitigation of the risks associated with these vulnerabilities are included in the links within the alert. COT is currently working to ensure that all the DNS servers maintained by COT are appropriately patched. Agencies with DNS servers not maintained by COT are advised that appropriate and timely patching on their DNS servers is urgent as well.

U.S. Cert - Vulnerability Note VU#800113

The Domain Name System (DNS) is responsible for translating host names to IP addresses (and vice versa) and is critical for the normal operation of internet-connected systems. DNS cache poisoning (sometimes referred to as cache pollution) is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching nameserver. DNS cache poisoning is not a new concept; in fact, there are published articles that describe a number of inherent deficiencies in the DNS protocol and defects in common DNS implementations that facilitate DNS cache poisoning. The following are examples of these deficiencies and defects:

- **Insufficient transaction ID space**
  The DNS protocol specification includes a transaction ID field of 16 bits. If the specification is correctly implemented and the transaction ID is randomly selected with a strong random number generator, an attacker will require, on average, 32,768 attempts to successfully predict the ID. Some flawed implementations may use a smaller number of bits for this transaction ID, meaning that fewer attempts will be needed. Furthermore, there are known errors with the randomness of transaction IDs that are generated by a number of implementations. Amit Klein researched several affected implementations in 2007. These vulnerabilities are described in the following vulnerability notes:

  - VU#484649 - Microsoft Windows DNS Server vulnerable to cache poisoning

  - VU#252735 - ISC BIND generates cryptographically weak DNS query IDs
  - VU#927905 - BIND version 8 generates cryptographically weak DNS query identifiers

- **Multiple outstanding requests**
  Some implementations of DNS services contain a vulnerability in which multiple identical queries for the same resource record (RR) will generate multiple outstanding queries for that RR. This condition leads to the feasibility of a 'birthday attack,' which significantly raises an attacker's chance of success. This problem was previously described in VU#457875. A number of vendors and implementations have already added mitigations to address this issue.

- **Fixed source port for generating queries**
  Some current implementations allocate an arbitrary port at startup (sometimes selected at random) and reuse this source port for all outgoing queries. In some implementations, the source port for outgoing queries is fixed at the traditional assigned DNS server port number, 53/udp.

Recent additional research into these issues and methods of combining them to conduct improved cache poisoning attacks have yielded extremely effective exploitation techniques. Caching DNS resolvers are primarily at risk--both those that are open (a DNS resolver is open if it provides recursive name resolution for clients outside of its administrative domain), and those that are not. These caching resolvers are the most common target for attackers; however, stub resolvers are also at risk.

Because attacks against these vulnerabilities all rely on an attacker's ability to predictably spoof traffic, the implementation of per-query source port randomization in the server presents a practical mitigation against these attacks within the boundaries of the current protocol specification. Randomized source ports can be used to gain approximately 16 additional bits of randomness in the data that an attacker must guess. Although there are technically 65,535 ports, implementers cannot allocate all of them (port numbers <1024 may be reserved, other ports may already be allocated, etc.). However, randomizing the ports that are available adds a significant amount of attack resiliency. It is important to note that without changes to the DNS protocol, such as those that the DNS Security Extensions (DNSSEC) introduce, these mitigations cannot completely prevent cache poisoning. However, if properly implemented, the mitigations reduce an attacker's chances of success by several orders of magnitude and make attacks impractical.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Commonwealth Office of Technology
Security Administration Branch
120 Glenn’s Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServices@ky.gov
http://technology.ky.gov/security/